Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
IP-Enabled Services	)	WC Docket No. 04-36
	)	
E911 Requirements for IP-Enabled Service Providers	)	WC Docket No. 05-196
	)	
	)	

COMMENTS OF THE TEXAS COMMISSION ON STATE EMERGENCY COMMUNICATIONS

Gabriel Garcia
Assistant Attorney General
Office of the Attorney General of Texas
300 W. 15th Street, WPC Bldg., Floor 9
Austin, Texas 78701
512-936-1660
512-322-9114 (fax)
gabriel.garcia@oag.state.tx.us

ATTORNEYS FOR THE TEXAS COMMISSION ON STATE EMERGENCY COMMUNICATIONS

August 15, 2005

TABLE OF CONTENTS

The Texas Commission on State Emergency Communications ("TX-CSEC") files these comments in response to the Commission's Order and Notice of Proposed Rulemaking ("NPRM") in the above-captioned proceeding establishing E911 requirements for Voice over Internet Protocol ("VoIP") providers interconnected to the public switched telephone network ("PSTN").[1]

I. Introduction and Overview

TX-CSEC supports the requirements imposed by the *Order* and submits that the states have a critical role to play in order to achieve the desired implementation of E911 capability by interconnected VoIP providers. To this end, TX-CSEC supports the requirement that implementation be in accordance with standards that are being developed by the National Emergency Number Association ("NENA").[2] TX-CSEC has organized a Working Group of stakeholders to establish a process for implementation of the Commission's *Order* consistent with the developing *VoIP i2 Solution*.

Beyond the importance of state involvement in the implementation process, TX-CSEC believes that policy and technical issues raised in the NPRM should be addressed faithful to the principles that any obligations should be consistent with customer expectations regarding the service and should minimize changes to the existing 911 Network. TX-CSEC urges the Federal Communications Commission ("Commission") to

[1] *IP-Enabled Services; E911 Requirements for IP Enabled Service Providers*, WC Docket No. 04-36; WC Docket No. 05-196, First Report and Order and Notice of Proposed Rulemaking, 20 FCC Rcd 10245 (2005) ("*Order*"); 70 Fed. Reg. 37273 (June 29, 2005) (to be codified at 47 C.F.R. pt. 9).

[2] *Draft NENA Standards for VoIP/Packet Migration i2 Solutions (Working Draft – Includes Architecture Section and High-Level Interface Sections)*, NENA Template for Creating Or Updating E9-1-1 Standards Documents, Issue I DRAFT, April 22, 2005, prepared by NENA Technical Committee Chairs. ("*VoIP i2 Solution"*) ("The initial standards development work of the NENA VoIP/Packet Committee was to be completed by the end of 1Q05. This architecture embodies that initial work." *VoIP i2 Solution* at ¶ 1.2.)

establish reporting and state/federal enforcement policies to promote public safety and enhance the implementation process.

The Commission can further assist states in the implementation process by clarifying policies and/or passing additional regulations to address fee collection and remittance (which are of particular importance given the nomadic and non-native numbering features available through VoIP), protection of customer privacy, and access for disabled customers.

II. States Have a Critical Role to Play in the Implementation of E911 Capability of Interconnected VoIP Providers

The states have a critical role to play in the implementation of E911 capability by interconnected VoIP providers. This is only the latest event in the evolution of 911/E911 delivery. The implementation of this life saving service has been historically driven by state and local needs and resources—a characteristic that is not changed by the delivery of E911 by interconnected VoIP providers. The Commission acknowledged the "historic and important role" that states and localities have played in "creating and regulating 911/E911 operations … even in the context of wireless services."[3] There should be no legal or policy reasons to depart from the historic role states and localities have played in 911/E911 implementation. Texas has continued this important legacy as VoIP providers have entered the voice communications market.

Earlier this year, TX-CSEC established a VoIP 911 Working Group ("Working Group") to study how interconnected VoIP providers may impact E911 service – this was the outcome of a VoIP Forum organized by TX-CSEC in March 2005. Since the

[3] NPRM at ¶ 61. (The scope of states' involvement in the implementation of E911 by interconnected VoIP providers is addressed throughout these comments.)

Commission issued its *Order*, the Working Group has expanded the scope of its work to focus on the coordination of activities necessary to facilitate implementation of the *Order* in Texas. The Working Group consists of representatives from local 911 authorities from across the state, interconnected VoIP providers, incumbent and competitive local exchange companies ("ILECs" and "CLECs," respectively), 911 database providers, third-party vendors, and other stakeholders.

The Working Group met in mid-June 2005 and established committees in the following areas: (1) operations standards and procedures; (2) database implementation (including customer information validation process); (3) revenue impact; (4) contracts; and (5) rulemaking proceeding. The operations, database, revenue impact and contract committees are actively pursuing strategies intended to allow interconnected VoIP providers to meet the deadlines in the *Order*. Additionally, these committees will be making recommendations to the rulemaking committee in order to develop a comprehensive set of administrative procedures detailing the responsibilities of VoIP providers and other affected parties regarding the provisioning of effective E911 to VoIP customers.

The work of the operations and database committees has centered on implementation of VoIP E911 capability consistent with the *VoIP i2 Solution* architecture. Several members of these committees are active participants in industry groups that have been developing the *VoIP i2 Solution* standards over the last two years. The contracts committee is developing model contracts to provide interconnected VoIP providers with the authority to access the dedicated 9-1-1 network. The revenue committee is assessing issues related to the financial impact of providers and their

customers having access to the network. Finally, the rulemaking committee intends to incorporate the recommendations from the other four committees into a draft rule that is expected to be published for comment in late September 2005.

III. Policy and Technical Issues Should Be Addressed Following the Principles that Any Recommendations Should Be Consistent with Customer Expectations and Service Functionality and Should Minimize Changes to the Existing 911 Network

TX-CSEC believes that recommendations to the technical and policy issues raised in the NPRM should minimize changes to the existing emergency services infrastructure. For instance, the NPRM asks whether E911 obligations should be extended to VoIP providers that are not fully interconnected to the PSTN, i.e., should E911 obligations apply to VoIP services that enable users to terminate calls to the PSTN but do not permit users to receive calls that originate on the PSTN, and vice-versa[4]

The guiding principles for determining whether E911 obligations should be extended to VoIP providers that are partially interconnected with the PSTN, and others, are customer expectations and service functionality. TX-CSEC agrees with the Commission's conclusion that it is reasonable for "customers [to] expect that VoIP services that are interconnected with the PSTN will function in some ways like a 'regular telephone' service," particularly with regards providing access to emergency services by dialing 911.[5] To the extent that the same customer expectations apply to VoIP services partially interconnected with the PSTN, the same E911 requirements should apply.

Similarly, the Commission asks whether E911 obligations should apply to IP-based voice services that do not require a broadband connection.[6] Here again, the method

[4] NPRM at ¶ 58.
[5] 70 Fed. Reg. 37274.
[6] NPRM at ¶ *58.*

of transport is immaterial. The guiding principles are customer expectations and the intended functionality of the service. Accordingly, the *Order's* requirements should be extended to such a service.

The Commission also requested comment on whether providers of "wireless interconnected VoIP service [would] be more appropriately subject to our existing 911/E911 rules for CMRS."[7] At present there are no truly wireless VoIP providers. However, due to of the nomadic nature of VoIP, the Commission should develop CMRS-type rules to address financial issues such as determining the situs for applying state emergency service fees/surcharges, irrespective of whether the interconnected VoIP provider offers wireline or wireless services.

Regarding the requirements for customer updates of their registered location, the Commission states that it expects users to update their registered location immediately. If this is not feasible, however, what performance standards should the Commission adopt regarding the length of time between when an end user updates registered location information and when the service provider takes the actions necessary to enable E911 from the new location?[8] TX-CSEC believes that a customer should have access to emergency services immediately upon the VoIP service becoming functional—the customer having provided the registered location as part of the subscription process. When a customer changes or updates the registered location once service has been activated, E911 capability should be in place within 24 hours of such an update. This is consistent with the standard that applies to wireline telecommunications carriers in Texas. To the extent that E911 obligations for interconnected VoIP providers mirror existing

[7] NPRM at ¶ 59.
[8] *Id*. at ¶ 59.

standards for other providers connecting to the 911 Network, changes to the network will be minimized.

In a related question, the Commission asked how registered locations that are not associated with a street address should be treated.[9] TX-CSEC supports the requirement that registered locations should be "civil locations" in the nature of physical postal addresses and that they be validated against the Master Street and Address Guide ("MSAG"). This approach is consistent with the *VoIP i2 Solution*.[10] Interconnected VoIP providers must be required to send appropriate, readable, MSAG valid, civil location information to the PSAP, just as it is required of wireline communications providers. To do otherwise would merely shift the burden to PSAPs (possibly at the time of an emergency) when they have neither the resources nor a relationship with the customer to facilitate the registration process. Admittedly, this approach requires that accurate addressing information be made freely available to interconnected VoIP providers, which is a responsibility shared by the 9-1-1 entities.

Other issues that need further consideration in the VoIP context relate to other emergency and non-emergency telephone numbers, such as 1-800 poison control center calls, 2-1-1, and 3-1-1. These emergency and non-emergency service providers may transfer calls to or receive 9-1-1 transfer calls from PSAPs. Correct routing of such calls is important in order to maintain the usefulness of such numbers in a VoIP environment. Additional Commission attention to and clarification on these types of issues would be appropriate.

---

[9] *Id*.
[10] *VoIP i2 Solution* at ¶ 2.4.

IV. The Commission Should Establish Reporting Requirements and State/Federal Enforcement Policies that Promote Public Safety

The Commission should establish certain reporting requirements for interconnected VoIP providers and develop state/federal enforcement policies in order to promote public safety. The Commission asks whether it should impose reporting obligations on VoIP providers beyond the compliance letter referenced in the *Order*.[11] TX-CSEC recommends that the Commission require interconnected VoIP providers to report to the Commission—and make available to the states—their serving areas, implementation progress, and identify their relationships with VoIP enablers such as VoIP Positioning Centers ("VPC"), Emergency Services Gateway ("ESGW"), database providers, CLECs, and ILECs. Imposing minimal reporting requirements is invaluable to ensuring that the 9-1-1 community is able to continue meeting consumer expectations when the numbers 9-1-1 are dialed.

The Commission should also develop a cooperative state/federal enforcement policy that gives both state and federal authorities' latitude to bring enforcement actions. The Commission, of course, has enforcement authority over violations to its rules. However, the Commission should not seek to preempt related state enforcement actions that would arise from violations of state statutory and regulatory requirements that apply in a nondiscriminatory fashion to all providers interconnected to the 9-1-1 Network.

V. The Customer's Primary Place of Use Should Determine Liability for State 911 Service Fees and Surcharges for Nomadic and Static Customers

The Commission can assist the states with the implementation of E911 capability by establishing a clear policy regarding the proper situs for purposes of determining

[11] NPRM at ¶ 60.

liability for 911 fees and surcharges. In the VoIP service market there has been debate regarding what state or local jurisdiction should assess 911 service fees given the nomadic nature of VoIP and the ability for customers to obtain a non-native NXX number resources. Given that these issues arise as a result of the nomadic nature of VoIP, much as it did with respect to mobile communications, TX-CSEC recommends that the statutory requirements for sourcing charges for mobile telecommunications services (4 U.S.C. §§ 116 – 126) be made applicable to interconnected VoIP providers.

VI. The Commission Should Establish Clear Customer Privacy Protection Policies

Pursuant to its ancillary authority, the Commission should establish clear customer privacy protection policies to prevent the unintended disclosure of personal customer information. In the NPRM, the Commission surmises that when the E911 rules are fully implemented, they "will require interconnected VoIP providers to transmit a customer's Registered Location to an appropriate PSAP, which necessarily requires providers of such services to maintain a list of their customers' Registered Locations, and makes that information available to public safety professionals and others when the customer dials 911."[12] This is not necessarily the case.

The *VoIP i2 Solution* addresses customer privacy and network security issues in several respects that may diminish some of the Commission's concerns. For instance, the *VoIP i2 Solution* contemplates the creation of a Valid Emergency Services Authority ("VESA") to ensure that only trusted entities with existing relationships will be provided access to E911 data and services. VESA uses authentication – the process of verifying the claimed identity of a session requester – as a security measure to access E911 data.

[12] NPRM at ¶ 62.

Other security measures built into the *VoIP i2* Solution architecture include (1) message integrity mechanisms to protect against unauthorized message modifications; (2) message encryption which is a process of disguising a message in such a way as to hide its substance from entities that do not posses an encryption key to read the message; and (3) application of network elements security measures, such as the ability to authenticate users, control user access privileges, initiate audit trails, report security alarms, recovery from intrusions, and minor data and system integrity.[13]

Moreover, under the *VoIP i2 Solution*, customer location information need not be maintained by the interconnected VoIP providers. Location information is vital for the delivery of emergency services. After location information has been determined and validated, the location information must be made available for routing an emergency call to the appropriate interconnected point and for delivery to the PSAP. The *VoIP i2 Solution* architecture contemplates two methods for storing customer location information that does not involve the interconnecting VoIP provider maintaining a list of customer registered locations. Option one is for the location information to be stored with the VoIP Endpoint Equipment – access to which might be maintained by an information technology ("IT") administrator for an enterprise, or an Internet Service Provider ("ISP") or access provider for a residential customer. Under this scenario, location and related mapping information is downloaded to the appropriate entities when a 911 call is made.[14] The second option is for a third-party referred to as the Location Information Server ("LIS") to serve as the repository for location information. Under this option, the LIS stores location and related mapping information for a given VoIP

[13] *VoIP i2 Solution* at ¶¶ 3.1 – 3.7.
[14] *Id*. at ¶ 2.6.1.

Endpoint and provides the Endpoint a Location Key ("LK"). When a 911 call is made, the VoIP Endpoint will transmit the LK as the call is routed to the appropriate PSAP. Another entity on the daisy chain will use the LK to retrieve the location and information from the LIS and transmit it the PSAP.[15]

While these options provide some measure of protection for customer privacy, they do not create legal liability for entities that maliciously disclose customer information. Moreover, the majority of the security concerns for the *VoIP i2 Solution* are focused on ensuring that location information is accurate, valid, authentic, and associated with a specific call instance. "While secrecy and privacy of location may be of some importance, these are deemed secondary to routing and PSAP requirements."[16] In addition, the Commission may not have jurisdiction over the entities that would store customer location information under the *VoIP i2 Solution* architecture (IT administrators, ISPs, or the LIS). While there may be existing customer privacy legal protections that apply to ISPs, they do not necessarily extend to other entities that may serve of repositories of customer location information in the future. This may be an area that Congress should address with new customer protection legislation designed to extend to VoIP customers similar protection as customer proprietary network information ("CPNI") rules which currently apply to telecommunications services.

For its part, the Commission should use its ancillary jurisdiction over interconnected VoIP providers to establish that customer information in their possession may not be disclosed to third parties for non-emergency delivery purposes.

[15] *Id*. at ¶¶ 2.3.8 and 2.6.2.
[16] *Id*. at ¶ 3.7.

VII. The Commission Should Ensure that Customers with Disabilities Can Reach 911 Service Through Interconnected VoIP Providers

The Commission also seeks comments on whether persons with disabilities can use interconnected VoIP service to directly call a PSAP via a TTY in light of the requirement in Title II of the Americans with Disabilities Act that PSAPs be directly accessible by TTY.[17] Simply put, yes. The multi-functional nature of IP technology holds great promise for advanced communications services for customers with disabilities. However, unless interconnected VoIP providers are required to meet the same TTY standards that apply to other voice providers, market entry of those advanced IP technologies for disabled customers will be delayed or may not materialize. This requirement would be an important step in that direction.

VIII. Conclusion

TX-CSEC appreciates this opportunity to comment in this important proceeding. As the Commission works toward implementing the *Order*, TX-CSEC will continue to be engaged in the implementation process in Texas and urges the Commission to adopt additional rules consistent with the recommendations outlined above.

G:\Sharedfiles\PAR\CSEC\VoIP 911 Comments 081505.doc

[17] NPRM at ¶ 63.